

Path Discovery & Validation (PD-VAL) Working Group

Minutes of the 13 October 2005 Meeting

NIST North Building, West Diamond Avenue, Gaithersburg MD 20878/ Room 618

A. AGENDA

- 1) Welcome & Opening Remarks / Introductions
- 2) Overview of Vendor Test Results
- 3) Validation Methodology & Criteria
- 4) GSA's Validation Demo Update
- 5) Entrust Presentation
- 6) Other Topics
- 7) Adjourn Meeting

B. ATTENDANCE LIST

Organization	Name	Email	Telephone
Department of Commerce (NIST) PD-VAL Co-Chair	Cooper, David	david.cooper@nist.gov	301-975-3194
Department of State (Mount Airey Group)	Russell, William	russellwc@mountaireygroup.net	571-334-1671
GSA/OGP	Giles, April	april.giles@gsa.gov	Teleconference
FPKI OA Program Manager/PD-VAL Chair	Jenkins, Cheryl	cheryl.jenkins@gsa.gov	571-259-9923
NFC/USDA	Goodwin, Linda	linda.goodwin@usda.gov	Teleconference
FICC support (FC Business Systems)	Petrick, Brant	brant.petrick@gsa.gov	202-208-4673
Secretariat (Enspier Technologies)	Fincher, Judy	Judith.fischer@enspier.com	703-299-3444
Bridge-2-Bridge WG (Enspier Technologies)	Simonetti, David	david.simonetti@enspier.com	Teleconference
FPKI OA (Mitrotek)	Lins, Andrew	andrew.lins@mitrotek.org	Teleconference
Tumbleweed (vendor)	Ebbets, Steve	Steve.Ebbets@TUMBLEWEED.COM	Teleconference
Tumbleweed (vendor)	Smith, Ann		Teleconference
Tumbleweed (vendor)	Futrell, John		Teleconference
Tumbleweed (vendor)	Ray, Katie		Teleconference
SRA	Ganta, Tin2	Tin2_ganta@sra.com	Teleconference
Department of Defense	Mitchell, Deborah M.	dmmitc3@MISSI.NCSC.MIL	Teleconference
Department of State	Edmonds, Deborah D.	EdmondsDD@STATE.GOV	202-647-9175
Orion (vendor)	Shorter, Scott	sshorter@orionsec.com	
Electrosoft Services	Gupta, Sarbari	sarbari@ELECTROSOFT-INC.COM	703-918-4905
CoreStreet, Ltd. (vendor)	Dulude, Bob	bob@corestreet.com	Teleconference
CoreStreet, Ltd. (vendor)	Briley, Jr, James	jbriley@corestreet.com	301.318.5096
CoreStreet, Ltd. (vendor) Director Defense & Intelligence Programs	Townsend, Paul J.	ptownsend@corestreet.com	301-908-0293 (Cell) 301-865-6360 (office)

Organization	Name	Email	Telephone
Entrust (vendor)	Gopal, Gautam	Gautam.gopal@entrust.com	703-269-2023
DOJ	Young, Siegfroid	Siegfried.young@usdoj.gov	202-616-8989

C. MEETING ACTIVITY

Agenda Item 1

Welcome & Opening Remarks / Introductions - Ms. Cheryl Jenkins

Ms. Cheryl Jenkins, FPKI OA Program Manager and PD-VAL Chair, called the meeting to order at 9:40 a.m. with attendee introductions.

Agenda Item 2

Overview of Vendor Test Results – Mr. David Cooper, NIST

The PD-VAL WG put out an RFI for COTS products that perform Path Discovery and Validation of certificates. There was a brief review of vendors who responded to the RFI and whose products are currently being tested in the E-Authentication Interoperability Lab:

- Tumbleweed Communications
- CoreStreet, Ltd.
- Orion Security Solutions
- Entrust

Mr. David Cooper, PD-VAL Co-Chair, described this testing.

Tumbleweed Communications

The test results for Tumbleweed testing were good. We tested the Microsoft IIS “plug-in” and encountered one issue. There was a discrepancy if you’re using a different “plug-in.” You get different results from the server compared to what the user sees. Tumbleweed is looking into it.

The advantage to using Tumbleweed is that you can buy the server and use any SCVP client. Ms. Jenkins noted that SCVP will be considered as “the protocol” for PD-VAL when it becomes available and widely adopted. Mr. Cooper stated that a stable RFC for SCVP may come out of the November IETF meeting in Vancouver.

CoreStreet, Ltd.

Mr. Cooper stated that the CoreStreet testing is moving along, but there are still configuration problems. CoreStreet will have a patch soon to address two configuration issues:

1. CRL Validation Tests should fail/safe rather than accepting the path
2. Segmented CRL’s (a security risk).

CoreStreet will make available other configuration options that won’t use segmented CRL’s.

Ms. Jenkins stated that the lab needs to retest the product with a different configuration that can verify that the certificate has not been revoked. This testing should be complete by October 28, she said, and the technical synopsis will be posted then. She noted that both CoreStreet and Tumbleweed will have local and hosted validation solutions.

Action: Mr. Bob Dulude (CoreStreet) is to provide the pricing information he submitted previously again.

Ms. Jenkins stated she is in touch with the Designated Approving Authority (DAA) for the Operational Research Consultants (ORC) and CyberTrust (BeTrusted) – the vendors providing hosted validation services for Tumbleweed and CoreStreet respectively. She is requesting that the DAA grants permission to leverage ORC’s and CyberTrust’s (BeTrusted) accreditations to host qualified PD-VAL products. She noted that some testing (e.g., penetration) maybe required for those vendors that do not already have a qualified product in their accredited environment.

Orion

No significant technical problems were found in the testing of Orion’s Webcullis version 1.0 and Security plug-in for IIS.

Orion’s web server plug-in supports both Apache on Windows platform and Microsoft's IIS, although Apache has not yet been tested.

The DoD has decided to offer this product as open source.

The discussion turned to issues regarding the configuration control management of an open sourced solution. The idea of licensing the solution and the possibility of Orion’s Webcullis becoming a COTS product were discussed. However, the details of this issue are still being worked out by Ms. Jenkins, along with Dr. Peter Alterman, Chairman of the FPKIPA, Ms. Judith Spencer and Mr. David Cooper. They will meet with the DoD to discuss these issues early November. They will report back at the next PD-VAL meeting (tentatively set for November 17).

Entrust

True Pass is currently being tested in the E-Authentication Interoperability Lab. There are configuration issues within the lab environment.

Agenda Item 3

Validation Methodology & Criteria – Ms. Cheryl Jenkins

Ms. Jenkins stated that this document, which seeks to formalize the validation process, will come out in draft later this month.

Agenda Item 4

GSA’s Validation Demo Update – Ms. April Giles, GSA

Ms April Giles of the GSA/OGP, who is leading this effort, reported that she has awarded a contract to Enspier to test the qualified products with E-Authentication applications. The contractor kick-off meeting has been held. There are no further updates available at this time and more information will be provided as it becomes available.

She asked that vendors or agencies that want to participate call her at 202-281-5305.

Agenda Item 5

Entrust Presentation – Mr. Gautam Gopal, Entrust

Mr. Gautam Gopal, Sales Engineer, Entrust (McLean, VA) made a PowerPoint slide presentation on the initial set of Entrust components that they plan to submit for testing at the E-Authentication Interoperability Lab. These are:

- True Pass
- Verification Server 7.0
- Entelligence Desktop Solutions 7.0 (EDS)
- Entrust Authority Java Toolkit 7.1 SP1 for the Java Platform

True Pass

This is a web product that does on-line PKI-based [client side] authentication and digital signatures. It supports Single Sign On and allows authentication locally at the desktop, not over the Internet like SSL. It is integrated with web forms and with Adobe and other document management solutions, such as Open Text and Hummingbird. It works with hardware tokens through CAPI.

The impetus behind True Pass testing is that the Department of Treasury wants to use it.

A discussion ensued on the architecture of True Pass and it was decided to schedule another meeting with the Entrust Product Manager, Alan McPhee. The PD-VAL Working Group needs to understand how the PD-VAL piece functions in order to determine how it will be tested.

Action: Ms. Cheryl Jenkins is to schedule a technical meeting with Entrust (Alan McPhee), David Cooper and herself.

Verification Server 7.0

This product gives you the ability to provide digital signatures, time stamp and encryption against XML data. It provides server-to-server authentication using XML objects. The Verification Server is currently being tested at the Department of State to digitally sign passports, but not for path validation.

There was discussion as to whether the Verification Server 7.0 is out of scope for PD-VAL testing. Ms. Jenkins suggested that she consult with the E-Authentication Program Office to determine if they want to test it. Otherwise, it is out of scope for the PD-VAL WG.

Entrust Authority Java Toolkit 7.1 SP1 for the Java Platform

Entrust is proposing this Java Toolkit for testing in the E-Authentication Interoperability Lab. It is a set of API's that perform PKI functions and is FIPS 140-2 certified.

Entelligence Desktop Solutions 7.0 (EDS)

This component was not built using the Java Toolkit and will need to be tested in the E-Authentication Interoperability Lab. It has the ability to manage Entrust-issued certificates on the user desktop and supports applications such as email, e-forms, VPN, etc. It is integrated with Adobe.

Agenda Item 6

Other Topics

The next meeting, previously scheduled for November 10, has been moved to November 17, but may not be held if the current round of testing is not completed.

Agenda Item 7

Adjourn Meeting

The meeting was adjourned at 11:15 a.m.

PD-VAL Current Action Items

No.	Action Statement	POC	Start Date	Target Date	Status
001	Put together a synopsis (written report) of Interoperability Lab testing status and results as of 9/15/05.	Cheryl Jenkins, David Cooper	Sept. 15, 2005	Oct. 13, 2005	Open
002	Contact Scott Shorter of Orion to get the Apache version of Webcullis into the interoperability lab.	Arthur Russell	Sept. 15, 2005	Sept. 30, 2005	Open
003	Check with DoD on the use of Orion GOTS product(s) by other federal agencies.	Deborah Mitchell	Sept. 15, 2005	Sept. 30, 2005	Open
004	Provide comment on the 11 August Minutes.	Cheryl Jenkins	Sept. 15, 2005	Sept. 16, 2005	Open
005	Schedule a technical meeting with Entrust (Alan McPhee) with David Cooper and Cheryl Jenkins	Cheryl Jenkins	Oct. 13, 2005	Nov. 17, 2005	Open
006	Mr. Bob Dulude (CoreStreet) is to provide the pricing information he submitted previously again.	Bob Dulude, CoreStreet	Oct. 13, 2005	Oct. 20, 2005	Open